

Docket No.: 27592-01057-US3  
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

---

In re Patent Application of:  
Hans Wyssen

Application No.: 10/582,831

Confirmation No.: 4997

Filed: April 12, 2007

Art Unit: 2431

For: A METHOD AND SYSTEM FOR VERIFYING  
DOCUMENTS

---

Examiner: K. Abrishamkar

**APPEAL BRIEF**

MS Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This brief is filed in furtherance of a Notice of Appeal filed on September 8, 2010. Appellant believes that any fees required in conjunction with this submission are indicated on an accompanying paper. However, should any further fees be due, Appellant authorizes such fees to be charged to Deposit Account No. 22-0185, under Order No. 27592-01057-US3, from which the undersigned is authorized to draw.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205 which begin on the pages as indicated:

I.	Real Party in Interest .....	3
II.	Related Appeals, Interferences, and Judicial Proceedings .....	4
III.	Status of Claims .....	5
IV.	Status of Amendments.....	6
V.	Summary of Claimed Subject Matter .....	7
VI.	Grounds of Rejection to be Reviewed on Appeal .....	10
VII.	Argument .....	11
VIII.	Claims Appendix .....	19
IX.	Evidence Appendix .....	24
X.	Related Proceedings Appendix .....	25

## **I. REAL PARTY IN INTEREST**

The real party in interest for this appeal is the Thayn Firm, LLC.

## **II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS**

There are no other appeals, interferences, or judicial proceedings which, to the best of Appellant's knowledge, will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

### **III. STATUS OF CLAIMS**

#### **A. Total Number of Claims in Application**

There are 38 claims pending in this application.

#### **B. Current Status of Claims**

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-38
4. Claims allowed: None
5. Claims rejected: 1-38

#### **C. Claims on Appeal**

The claims on appeal are 1-38.

#### **IV. STATUS OF AMENDMENTS**

All prior amendments were entered. The claims included in the attached Claims Appendix reflect each of the prior amendments.

## **V. SUMMARY OF CLAIMED SUBJECT MATTER**

The following summary sets forth exemplary reference characters and pages and line numbers in the subject application where an embodiment of the present invention is illustrated or described. The identification of reference characters and pages and line numbers does not constitute a representation that any claim element is limited to the embodiment illustrated at the reference character or described in the referenced portion of the specification.

The application includes three independent claims. Independent Claims 1 and 38 are directed to systems and independent Claim 19 is directed to a method.

### **A. Summary of the Embodiment of Claim 1**

An embodiment of the present invention is directed to a computer system. *See, e.g., Specification, pg. 2, ll. 27-28.* In the system, documents including, for example, certificates, diplomas, deeds, contracts, photos, legal documents and the like are collected by a central repository. *See Specification, pg. 5, ll. 26-28.* For example, a paper document such as a diploma, certificate, or a notarized copy of a document or the like may be scanned using a scanner and posted to a website of the repository, to be accessed for authentication purposes by users through the internet. *See Specification, pg. 6, ll. 17-18.* Documents which are scanned may be carefully examined, by verification authority, and verification information generated. *See Specification, pg. 7, ll. 21-23.* The resulting verification information may be made available to persons who viewed selected scanned documents online. *See Specification, pg. 7, ll. 23-26.* The verification information may be presented to online viewers so as to appear on the electronic document image of the scanned document. *See Specification, pg. 9, ll. 20-24.* Verification information may relate to one or more elements of the document. *See Specification, pg. 8, l. 7.*

Consistently, Claim 1 recites:

- A computer system, comprising:
  - a memory configured to store:
    - electronic image data corresponding to an original tangible document, the tangible document having an electronic displayable verifiable provenance, and
    - separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance, and
  - an output configured to provide said image data and said

verification information for display by the user to authenticate the original tangible document,  
wherein the verification information is displayed on the image data.

## **B. Summary of the Embodiment of Claim 19**

An embodiment of the present invention is directed to a method of displaying a document for authentication. *See, e.g., Specification, pg. 3, ll. 17-18.* In the method, documents including, for example, certificates, diplomas, deeds, contracts, photos, legal documents and the like are collected by a central repository. *See Specification, pg. 5, ll. 26-28.* For example, a paper document such as a diploma, certificate, or a notarized copy of a document or the like may be scanned using a scanner and posted to a website of the repository, to be accessed for authentication purposes by users through the internet. *See Specification, pg. 6, ll. 17-18.* Documents which are scanned may be carefully examined, by verification authority, and verification information generated. *See Specification, pg. 7, ll. 21-23.* The resulting verification information may be made available to persons who viewed selected scanned documents online. *See Specification, pg. 7, ll. 23-26.* The verification information may be displayed to online viewers so as to appear on the electronic document image of the scanned document. *See Specification, pg. 9, ll. 20-24.* Verification information may relate to one or more elements of the document. *See Specification, pg. 8, l. 7.*

Consistently, Claim 19 recites:

A method of displaying a document for authentication, comprising:  
creating electronic image data corresponding to an original document, the original document having an electronic displayable verifiable provenance;  
providing electronic, displayable verification information corresponding to the electronic displayable verifiable provenance;  
and  
displaying the image data and the verification information, to permit a user to authenticate the original document,  
wherein the verification information is displayed on the image data.

## **C. Summary of the Embodiment of Claim 38**

An embodiment of the present invention is directed to a computer system. *See, e.g.,*



*Specification*, pg. 2, ll. 27-28. In the system, documents including, for example, certificates, diplomas, deeds, contracts, photos, legal documents and the like are collected by a central repository. *See Specification*, pg. 5, ll. 26-28. For example, a paper document such as a diploma, certificate, or a notarized copy of a document or the like may be scanned using a scanner and posted to a website of the repository, to be accessed for authentication purposes by users through the internet. *See Specification*, pg. 6, ll. 17-18. Documents which are scanned may be carefully examined, by verification authority, and verification information generated. *See Specification*, pg. 7, ll. 21-23. The resulting verification information may be made available to persons who viewed selected scanned documents online. *See Specification*, pg. 7, ll. 23-26. The verification information may be presented to online viewers so as to appear on the electronic document image of the scanned document. *See Specification*, pg. 9, ll. 20-24. Verification information may relate to one or more elements of the document. *See Specification*, pg. 8, l. 7.

Consistently, Claim 38 recites

A computer system comprising:

a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to authenticate the document, wherein the electronic signal comprises:

electronic image data corresponding to an original document having an electronic displayable verifiable provenance;  
and

electronic, displayable verification information corresponding to the provenance of at least part of the original document,

wherein the verification information is displayed on the image data.

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Claims 1-38 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,587,945 to Pasioka (hereinafter “Pasioka”) in view of U.S. Patent No. 7,295,677 to Simpson et al. (hereinafter “Simpson”).

## **VII. ARGUMENT**

The recited systems of Claims 1-17 and 38 and methods of Claims 19-37 are each patentable over the combination of Pasioka and Simpson, at least by virtue that Pasioka and Simpson fail to teach or suggest each of the recited limitations of any of these claims.

### ***A. Pasioka and Simpson Fail in Any Combination to Teach or Suggest the Recited Elements of Claims 1-18.***

Obviousness is a question of law that is evaluated based on underlying factual questions about the level of skill in the art at the time the invention was made, the scope and content of the prior art, and the differences between the prior art and the patent claim. *KSR Int'l Co. v. Teleflex, Inc.*, 127 S.Ct. 1727 at 1734, 1745 (2007), (quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966)).

The Examiner bears the burden of establishing a *prima facie* case of obviousness based upon the prior art. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). Appellant may traverse the Examiner's *prima facie* determination as improperly made out, and/or Appellant may present objective evidence tending to support a conclusion of non-obviousness. *In re Heldt*, 58 C.C.P.A. 701, 433 F.2d 808, 811, 167 USPQ 676, 678 (CCPA 1970). Appellant traverses the Examiner's *prima facie* determination as being improperly made out, and submits the evidence of record supports a conclusion of non-obviousness.

#### ***1. Pasioka and Simpson Fail in Any Combination to Teach or Suggest At Least the Recited "original tangible document ... having an electronic displayable verifiable provenance" of Claim 1.***

Claim 1 recites, *inter alia*, "a memory configured to store: electronic image data corresponding to an original tangible document, the tangible document having an electronic displayable verifiable provenance." Pasioka and Simpson, alone or in combination, fail to teach or suggest such a limitation.

For example, the appealed rejections assert that Pasioka teaches a memory configured to store image data corresponding to an original document having an electronic displayable verifiable provenance at col. 4, lines 13-18. *See, e.g., 11/3/2009, Office Action, pg. 3; 6/8/2010,*

*Office Action*, pg. 4. Appellant traverses this assertion for at least the following reasons.

Pasieka describes an author using an imager to create an image, which is automatically sent to a server which signs and stores the image. *See Pasieka*, col. 4, ll. 13-18. More particularly, the server as disclosed in Pasieka hashes the image record using a one-way hash to produce an image fingerprint. *See Pasieka*, col. 4, ll. 43-44. The server encrypts the image fingerprint using the server's private key (or author's or imager's private keys stored in the server) to form an image signature. *See Pasieka* col. 4, ll. 49-52.

Contrary to the appealed rejection assertions, an encrypted image fingerprint that merely serves as an image signature providing proof of authorship simply does not teach "separately derived electronic displayable verification information corresponding to the electronic displayable provenance," as recited in Claim 1. In Pasieka, the image signature corresponds to the image itself, rather than the "***electronic displayable verifiable provenance***" of the "[original] ***tangible document***," as recited in Claim 1.

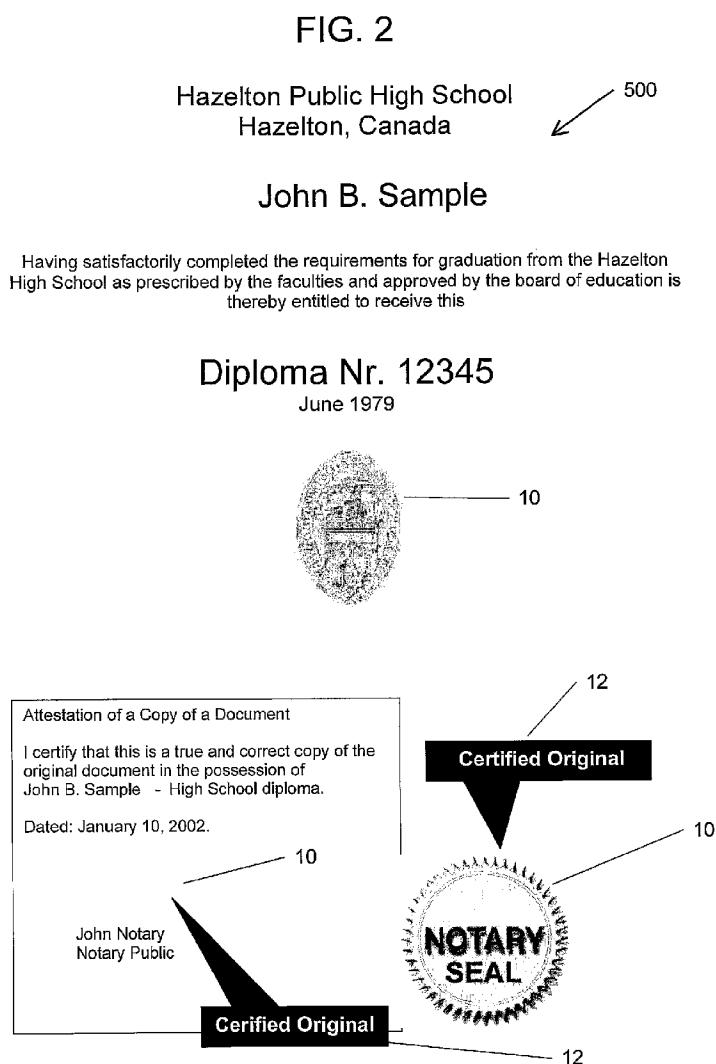
Further, the appealed rejections assert that Pasieka teaches an image that may be produced by a scanner and "has an electronically verifiable provenance as the transmission includes an author identifier and an imager device identification." *See, e.g., 6/8/2010 Office action*, pg. 2, "Response to Arguments", l. 7 – pg. 3, l. 2. However, Claim 1 does not call for any mere image and provenance, but rather explicitly recites "***an original tangible document ... having an electronic displayable verifiable provenance.***" Contrary to Claim 1, neither the image fingerprint nor the image signature, as described in Pasieka, is included in the original document. Further, even if, *arguendo*, the image results from a scan of an "original tangible document" as is alleged by the rejections, according to Pasieka, ***the original scanned document does not include the image signature***. Thus, the signature fails to even correspond to the recited original tangible document at all, no less the recited "***electronic displayable verifiable provenance***" included in the "[original] ***tangible document***," as recited in Claim 1.

Further, the appealed rejections appear to equate any document that may be perceived to the Claim 1 recited, "original tangible document." *See, e.g., 6/8/2010, Office action*, pg. 2, "Response to Arguments", ll. 5-7. Appellant traverses this assertion as well.

Appellant acknowledges the PTO utilizes the "broadest reasonable interpretation" standard. *See, e.g., MPEP §2111*. However, claims must be interpreted in light of the specification and in view of one skilled in the art. *See, e.g., Phillips v. AWH Corp.*, 415 F.3d

1303, 75 USPQ 1321 (Fed. Cir. 2005); *see also, e.g., In re Cortright*, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999). And, “[t]he protocol of giving claims their broadest reasonable interpretation during examination does not include giving claims a legally incorrect interpretation.” *In re Skvorecz*, No. 2008-1221 (Fed. Cir. Sept. 3, 2009) at 8. Rather, “[t]his protocol is solely an examination expedient, not a rule of claim construction.” *Id.*

A non-limiting example of certain embodiments of the present invention may take the form of a “paper document” that includes indicia 10, and that is scanned to produce image data, such as is shown in Fig. 2 of the subject application (reproduced below).



In contrast to Claim 1, neither the Pasieka image fingerprint nor the Pasieka image signature are included in the original document. Rather, and as is explained by Pasieka itself, the

Pasieka server generates the image fingerprint and the image signature. Accordingly, it is improper to equate the Claim 1 recited, “[original] tangible document” to Pasieka’s “electronic image”, particularly since Claim 1 also recites “electronic image data corresponding to [the] original tangible document.”

Similarly deficient, Simpson merely proposes systems and methods for adding watermarks using network-based imaging techniques. *See Simpson, col. 3 l. 61 – col. 4 l. 8.* The Simpson watermark merely marks the primary image as the property of the owner (or marks the image in some other way, such as indicating that the primary image is a “draft” image). *See Simpson, col. 5, ll. 8-12.* Thus, like Pasieka the Simpson information merely relates to an image in general, rather than “*an original tangible document ... having an electronic displayable verifiable provenance,*” as recited in Claim 1.

Accordingly, Appellant respectfully requests reconsideration and removal of the rejection of Claim 1 for at least the foregoing reasons. Claims 2-18 depend on Claim 1 and therefore incorporate all of the elements of Claim 1, in addition to further limitations recited therein. Hence, Claims 2-18 are also allowable at least because of their dependence on Claim 1 and the additional elements set forth therein.

**2. *Pasieka and Simpson Fail in Any Combination to Teach or Suggest the Recited “separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance” of Claim 1.***

As discussed above, it is improper to attempt to equate the Claim 1 recited, “[original] tangible document” to Pasieka’s “electronic image,” particularly since Claim 1 also recites “electronic image data corresponding to [the] original tangible document.”

However, even assuming, *arguendo*, Pasieka’s electronic image could be considered the recited “original tangible document,” the asserted combined Pasieka and Simpson teachings would nonetheless still fail to teach or even suggest the recited “separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance.”

By way of further non-limiting example, and as is described in connection with Fig. 2 of the subject application (reproduced above), verification information inserted by the repository onto the electronic image appears as indicia 12. *See Specification, pg. 9, ll. 31-32.* Marks 10,

which may include signatures, seals, date stamps, ink stamps, embossing that were manually applied to the paper document that was scanned, are flagged with indicia 12 so that persons viewing the electronic document online are informed which marks 10 are original. *See Specification, pg. 9, ll. 31-32.* Marks 10 which were photocopied or printed to the paper document which was scanned would not be flagged with indicia 12. *See Specification, pg. 10, ll. 23-25.* Fig. 2 shows one mark 10 which was not flagged with indicia 12 because it is not original but rather a photocopy. *See Specification, pg. 10, ll. 23-25.*

The appealed rejections assert Pasioka teaches separately derived electronic displayable verification information corresponding to the provenance at column 4, lines 49-55. *See, e.g., 11/3/2009 Office action, pg. 3, ll. 1-8.* Appellant traverses this assertion for at least the following reasons.

Pasioka fails to teach or suggest the recited provenance in the first place, such that it also necessarily fails to teach or suggest any verification information corresponding to it. Further, and as discussed above, the cited Pasioka passage discusses the server encrypting the image fingerprint using the server's private key (or author's or imager's private keys stored in the server) to form an image signature. *See Pasioka, col. 4, ll. 49-52.*

Claim 1 instead explicitly calls for “***separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance.***” As discussed above, a non-limiting example of such verification information is shown in Fig. 2 of the subject application, which includes indicia 12. *See, e.g., Specification, pg. 9, ll. 31-32.* Contrary to Claim 1, the Pasioka signature does not “***correspond[] to the electronic displayable verifiable provenance.***” Rather, it “provide[s] proof that the author is the originator of the image, and that the image has not been altered by others since it was signed.” *See Pasioka, col. 4, ll. 52-55.*

Accordingly, and contrary to the appealed rejections, Pasioka fails to teach or suggest at least “***separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance,***” as recited in Claim 1.

As stated above, Simpson is similarly deficient. For example, Simpson merely proposes systems and methods for adding watermarks using network-based imaging techniques. *See col. 3, l. 61 – col. 4, l. 8.* The Simpson watermark merely marks the primary image as the property of the owner (or marks the image in some other way, such as indicating that the primary image is a “draft” image). *See Simpson, col. 5, ll. 8-12.* Thus, like Pasioka the Simpson information merely

relates to an image in general, rather than a “*separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance*,” as recited in Claim 1.

In view of the above, the Examiner fails to establish a *prima facie* case of obviousness with respect to Claim 1, and the rejection of Claim 1 under 35 U.S.C. §103(a) is improper. Accordingly, Appellant respectfully requests reconsideration and removal of the rejection of Claim 1. Claims 2-18 depend on Claim 1 and therefore incorporate all of the elements of Claim 1, in addition to further limitations recited therein. Hence, Appellant also requests reconsideration and withdrawal of the rejections of Claims 2-18, at least by virtue of the ultimate dependency of these claims upon base Claim 1.

***B. Pasioka and Simpson Fail in Any Combination to Teach or Suggest the Recited Elements of Claims 19-37.***

Claim 19, while of differing scope than Claim 1, analogously recites:

A method of displaying a document for authentication, comprising:  
creating electronic image data corresponding to an original document, the original document having an electronic displayable verifiable provenance;  
providing electronic, displayable verification information corresponding to the electronic displayable verifiable provenance;  
and  
displaying the image data and the verification information, to permit a user to authenticate the original document, wherein the verification information is displayed on the image data.

For at least reasons similar to those discussed above in connection with Claim 1, Pasioka and Simpson fail to teach at least the recited “original document having an electronic displayable verifiable provenance” and “displayable verification information corresponding to the electronic displayable verifiable provenance” of Claim 19. Accordingly, the rejection of Claim 19 is improper as the Examiner fails to establish a *prima facie* case of obviousness with respect to Claim 19. Appellant requests reconsideration and withdrawal of the rejection of Claim 19. Appellant also requests reconsideration and withdrawal of the rejections of Claims 20-37, at least by virtue of the ultimate dependency of these claims upon base Claim 19.



***C. Pasioka and Simpson Fail in Any Combination to Teach or Suggest the Recited Elements of Claim 38.***

Claim 38, while of differing scope than Claim 1, analogously recites:

A computer system comprising:

a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to authenticate the document, wherein the electronic signal comprises:

electronic image data corresponding to an original document having an electronic displayable verifiable provenance; and

electronic, displayable verification information corresponding to the provenance of at least part of the original document,

wherein the verification information is displayed on the image data.

For at least reasons similar to those discussed above in connection with Claim 1, Pasioka and Simpson fail to teach at least the recited “original document having an electronic displayable verifiable provenance” and “displayable verification information corresponding to the provenance of at least part of the original document” of Claim 38. Accordingly, the rejection of Claim 38 is improper as the Examiner fails to establish a *prima facie* case of obviousness with respect to Claim 38. Thus, Appellant requests reconsideration and withdrawal of the rejection of Claim 38 for at least the foregoing reasons as well.

Appellant may not have presented all possible arguments or have refuted the characterizations of either the claims or the prior art as may be found in the Office Action. However, the lack of such arguments or refutations is not intended to act as a waiver of such arguments or as concurrence with such characterizations.

Dated: November 8, 2010

Respectfully submitted,

Electronic signature: /John Paik/

John Paik

Registration No.: 54,355  
CONNOLLY BOVE LODGE & HUTZ LLP  
1875 Eye Street, NW  
Suite 1100  
Washington, DC 20006  
(202) 331-7111  
(213) 687-0498 (Fax)  
Attorney for Appellant

## **VIII. CLAIMS APPENDIX**

1. A computer system, comprising:  
a memory configured to store electronic image data corresponding to an original document having an electronic displayable verifiable provenance, and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document, and  
an output configured to provide said image data and said verification information for display by the user to authenticate the original document,  
wherein the verification information is displayed on the image data.
2. A computer system according to Claim 1 wherein the image data has been obtained from an authenticated source, and the verification information includes data corresponding to the provenance of the authenticated source.
3. A computer system according to Claim 1 wherein data is fed to and from the memory under the control of a repository.
4. A computer system according to Claim 3 wherein the verification information comprises data concerning the provenance that has been subjected to authentication by the repository, and the verification information being configured to signal to the user that the repository provides such authentication.
5. A computer system according to Claim 2 wherein data stored in the memory cannot be altered by users.
6. A computer system according to Claim 3 including apparatus to receive the image data from a remote location.
7. A computer system according to Claim 1 including a scanner for scanning an original document to produce said image data.

8. A computer system according to Claim 1 including a repository agent including apparatus operable to send image data corresponding to an original image to the repository.
9. A computer system according to Claim 8 wherein the repository agent is operable to send the image data together with source authentication information to indicate to the repository that the image data has been sent from the agent.
10. A computer system according to Claim 1 wherein the verification information comprises predetermined accreditation indicia to be viewed by a user concurrently with the image data for authenticating individual parts of the original document.
11. A computer system according to Claim 1 wherein the verification information comprises accreditation data to be viewed by a user in a separate field associated with the image data for authenticating the original document.
12. A computer system according to Claim 1 wherein the image data and the verification information are stored in a common electronic file.
13. A computer system according to Claim 12 wherein the file is a PDF file.
14. A computer system according to Claim 1 including a server providing said memory and operable to host a website at which said image data and verification information is viewable by a user to authenticate the original document.
15. A computer system according to Claim 1 wherein said output is connected to the Internet.
16. A computer system according to Claim 1 wherein said image data and verification information in the memory is password protected so that the user can only gain access thereto by use of the password.

17. A computer system according to Claim 1 wherein the image data and the verification information corresponding to the original document when stored in the memory collectively has an individual addressable identity.
18. A method of operating a computer system according to Claim 1 to provide said image data and said verification information for display by the user to authenticate the original document.
19. A method of displaying a document for authentication, comprising:
  - creating electronic image data corresponding to an original document having an electronic displayable verifiable provenance;
  - providing electronic, displayable verification information corresponding to the provenance of at least part of the original document; and
  - displaying the image data and the verification information, to permit a user to authenticate the document,wherein the verification information is displayed on the image data.
20. A method according to Claim 19 including receiving the image data from an authenticated source, storing the image data for display, and creating the verification information for the received image, wherein the verification information includes data corresponding to the provenance of the authenticated source.
21. A method according to Claim 19 including authenticating the source of the image data.
22. A method according to Claim 18 including feeding the image data and the verification information to a memory under the control of a repository for display to users wishing to authenticate the original document.
23. A method according to Claim 22 wherein only the repository can change the data in the memory.

24. A method according to Claim 22 wherein the verification information comprises data concerning the provenance that has been authenticated by the repository.
25. A method according to Claim 24 wherein the repository communicates with the source of the image data to determine the provenance thereof and to develop said verification information.
26. A method according to Claim 22 including feeding the image data to the repository from a remote location.
27. A method according to Claim 22 including sending said image data corresponding to an original image from a repository agent to the repository.
28. A method according to Claim 26 including sending the image data together with source authentication information to indicate to the repository that the image data has been sent from the repository agent.
29. A method according to Claim 18 including configuring the verification information to include predetermined accreditation indicia viewable concurrently with the image data for authenticating individual parts of the original document by a user that authenticates the document.
30. A method according to Claim 18 including configuring the verification information to comprise accreditation data to be viewable by a user in a separate field associated with the image data for authenticating the original document.
31. A method according to Claim 18 including storing the image data and the verification information are stored in a common electronic file.
32. A method according to Claim 18 including storing the image data and the verification information are stored in a common electronic PDF file.

33. A method according to Claim 18 including hosting a website at which said image data and verification information is viewable by a user to authenticate the original document.
34. A method according to Claim 18 including authenticating the original document by viewing said electronic image data and the corresponding verification information.
35. A method according to Claim 18 wherein said image data and verification information is password protected so that a user can only gain access thereto by use of the password, and including supplying the password to a user to permit the user to authenticate the original document.
36. A method according to Claim 18 wherein the image data and the verification information corresponding to the original document collectively have an individual addressable identity and including supplying the individual addressable identity to a user to permit the user to access the data and information for authenticating the original document.
37. A method according to Claim 35 including supplying a hyperlink to the user.
38. A computer system comprising:  
a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to authenticate the document, wherein the electronic signal comprises:  
electronic image data corresponding to an original document having an electronic displayable verifiable provenance; and  
electronic, displayable verification information corresponding to the provenance of at least part of the original document,  
wherein the verification information is displayed on the image data.

## **IX. EVIDENCE**

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.



## **X. RELATED PROCEEDINGS**

No related proceedings are referenced in Section II above, so no Appendix is included.